フォレンジック解析報告書

対象ケース: CASE-SAMPLE-202611 ／ 作成日時: 2026-11-23 09:00 JST ／ 総合判定: 緊急 ／ 検知数: 4 件

総合判定: 緊急

極めて危険度の高い異常が検知されました。被害範囲の特定と封じ込めを直ちに実施してください。

今すぐやること（最優先）

[ ] (1) 影響端末 SRV-FILE01 をネットワークから切り離す（電源は切らず隔離機能を優先）

[ ] (2) アカウント svc_backup のパスワードを直ちに変更・無効化し、外部からのRDP接続を遮断する

判定の理由: 緊急検知 1 件、高リスク検知 2 件、認証情報の不正利用疑い

目次

1. 何が起きたか（要約）
2. 影響を受けた範囲
3. 時系列で見る流れ
4. 対応チェックリスト
5. 調査の限界・追加確認が必要な点
6. 用語集
7. 付録（技術者向け）

1. 何が起きたか（要約）

危険度	件数	対応の目安
緊急	1 件	直ちに対応が必要
高	2 件	早急に確認が必要
中	1 件	計画的に確認
低	0 件	通常運用との切り分け対象
合計	4 件	同じ出来事を複数視点で検知した重複を含みます

確認された主な出来事（同一事象を名寄せして表示）

- [緊急] 認証情報メモリ参照（LSASS）の疑い — 管理者権限アカウント svc_backup により、認証情報を扱う lsass.exe への読み取りアクセスが記録されました。
- [高] 外部からの遠隔ログイン成功（RDP） — 社外IP 198[.]51[.]100[.]42 から共有保守アカウント svc_backup でリモートデスクトップ接続が成功しました。
- [高] 不審な定期実行タスクの登録 — 深夜時間帯に C:¥ProgramData¥Updater¥sync.ps1 を起動するスケジュールタスクが新規登録されました。
- [中] 一時フォルダへの圧縮ファイル作成 — 業務共有資料を対象とした 7z アーカイブ作成（C:¥Users¥tanaka.taro¥AppData¥Local¥Temp¥export_202611.7z）を検知しました。

2. 影響を受けた範囲

項目	確認内容
確認された端末	計 1 台: SRV-FILE01
関連アカウント	計 2 件: svc_backup, tanaka.taro
記録データの期間	2026-11-20 ～ 2026-11-21（証跡内の最古～最新の記録期間であり、解析実施日ではありません）

3. 時系列で見る流れ

時刻は日本時間（JST）です。同じ月内で内容が完全に重複する記録は回数をまとめて表示しています。

2026-11

- 2026-11-20T14:12:08Z 外部IP 198[.]51[.]100[.]42 から svc_backup への遠隔ログイン成功（EventID 4624）
- 2026-11-20T14:18:45Z 新規スケジュールタスク ¥Microsoft¥SyncJob 登録（EventID 4698）
- 2026-11-20T14:25:19Z lsass.exe プロセス参照の異常イベント（EventID 4656）
- 2026-11-20T14:41:02Z 一時領域への 7z 圧縮ファイル作成（export_202611.7z）

4. 対応チェックリスト

今すぐ（24時間以内）

- [ ] 影響端末 SRV-FILE01 をネットワークから切り離す（電源は切らず隔離機能を優先）
- [ ] アカウント svc_backup のパスワードを直ちに変更・無効化し、外部からのRDP接続を遮断する

1～2週間以内

- [ ] スケジュールタスク ¥Microsoft¥SyncJob および sync.ps1 の作成経緯を確認・除去する
- [ ] 社内ファイアウォール・VPNの同時刻ログを確認し、198[.]51[.]100[.]42 および 203[.]0[.]113[.]77 との通信量を突き合わせる

追加確認（状況把握）

- [ ] LSASS 参照（11/20 23:25 JST）前後の管理者操作に心当たりがあるか担当者に確認する

5. 調査の限界・追加確認が必要な点

通常業務との切り分け対象・除外設定

- 許可リストによる自動除外: 0 件（提出ログ12,480件すべてを監査対象として保持）

調査の制約とご留意点

- 提出ログ範囲外の端末・ネットワーク機器（VPN / FW / プロキシ）の通信実績は直接確認できていません。

- 本解析は決定論的ルールエンジンによる自動照合結果です。正規の保守作業か否かは運用記録と照合してください。
- プライバシー保護のため、IPアドレス・個人を特定できるフォルダパス等は自動的に伏せて（[匿名化]）います。

6. 用語集

用語	わかりやすい説明
RDP（リモートデスクトップ）	離れた場所から別のWindows端末の画面を操作する機能です。不正アクセス経路になりやすいため確認が重要です。
Prefetch / cron	PrefetchはWindowsがプログラム実行を記録する仕組み、cronはLinux等で定期的に処理を自動実行する設定です。

7. 付録（技術者向け）

検知された攻撃の分類（MITRE ATT&CK;）

分類	件数	関連手法ID
初期アクセス	1 件	T1078
永続化	1 件	T1053.005
資格情報アクセス	1 件	T1003.001
収集	1 件	T1560.001

技術的な侵害指標（IoC 一覧）

種別	観測値
通信先・IP	198[.]51[.]100[.]42
通信先・IP	203[.]0[.]113[.]77
関連ファイル	C:¥ProgramData¥Updater¥sync.ps1
関連アカウント	svc_backup

解析した記録データの内訳

Windowsイベントログ: 9820 件 ／ プログラム実行痕跡: 1840 件 ／ Linux認証ログ: 820 件

データの取り扱い・証拠保全

- 外部AI非送信・プライバシー保護: 解析は決定論的ルールエンジンおよび統計処理のみで完結し、外部AI（LLM）へログや証跡を一切送信しません。
- 保管期限: 作成から 24 時間で完全廃棄（生データは処理完了後に即消去・最小限の問い合わせ対応用管理メタデータのみ別保管）。
- 証拠の改ざん防止記録: 記録数 6 件 ／ 整合性確認: 正常（OK） ／ 先頭ハッシュ: 9f86d081884c7d65…